

Verizon records show that CLECs employees and contractors have deliberately defeated security barriers on several occasions. This has included taping doors and tying door latches so that a door can be accessed without a card or keys.

53. To improve the effectiveness of card readers, cameras can help in the effort to verify that the person using the card actually owns the card, or to provide a visual record when unauthorized individuals use access cards. Again, this provides only an after-the-fact remedy, and significantly raises costs.

54. In short, using partitioning material in conjunction with cameras and card reader – as Verizon does -- is much more effective (and less costly) than using cameras and card readers alone. Thus, denying Verizon the ability to partition its equipment from the CLECs' equipment would not only jeopardize the security of the network, it would greatly increase the cost of maintaining security in a central office.

**D. UNESCORTED ACCESS TO REMOTE TERMINALS WILL ALLOW
ADDITIONAL SECURITY BREACHES.**

55. Securing remote terminals is even more problematic. These remote terminals house much of the same costly and delicate equipment housed in a central office, and present the same opportunities for service disruption, and equipment tampering and theft discussed above.

56. As Exhibit 10 to Attachment C-1 demonstrates, it is not possible to partition equipment in the small remote terminals. Moreover, Verizon has over 38,000 remote terminals; it plainly would not be feasible to install card readers and cameras in each of these locations, even assuming that these security methods worked – which they do not for the reasons discussed above. The only way to ensure adequate security at a

remote terminal is to allow the ILEC to require a security escort for the CLEC technicians or to limit remote terminals to virtual collocation.

IV. CONCLUSION

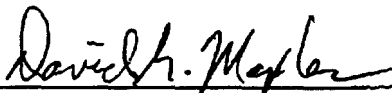
57. If Verizon is not permitted to separate or partition CLEC equipment, then the CLEC employees will have unlimited access to Verizon's equipment and network. Permitting such access creates significant risks for Verizon, its customers, and the communities served by Verizon's central offices.

58. The only truly effective way of ensuring the security and integrity of Verizon's network is to permit Verizon to fence off its equipment from CLEC equipment. As Exhibit 2 to Attachment C-1 and Attachment C-2 illustrate, partitioning is a reasonable method of security, is inexpensive, and does not occupy large amounts of floor space. Security cameras and card readers alone do not and cannot provide adequate security.

59. Finally, because it is impossible to secure remote terminals, only virtual collocation or escorted access should be permitted at these locations.

I declare under penalty of perjury under the laws of the United States of America
that the foregoing is true and correct.

Executed on October 12, 2000



David G. Maples

Before the
FEDERAL COMMUNICATIONS COMMISSION
 Washington, D.C. 20554

In the Matter of)	
)	
Deployment of Wireline Services Offering)	CC Docket No. 98-147
Advanced Telecommunications Capability)	
)	
and)	
)	
Implementation of the Local Competition)	CC Docket No. 96-98
Provisions of the Telecommunications)	
Act of 1996)	

ATTACHMENT C-1 TO THE DECLARATION OF DAVID G. MAPLES, III

1. On September 25, 2000, I visited a Verizon central office and a remote terminal, both located in Virginia. The following pictures were taken under my supervision to demonstrate several of the arguments I raise in my Declaration. These images show the significant risks that Verizon would face if it were prohibited from partitioning its equipment and network. I also demonstrate with these pictures that securing remote terminals is technically infeasible and cost prohibitive.

A. COMMINGLED EQUIPMENT CANNOT BE SECURED.

2. The Commission asked parties to analyze whether commingled equipment, *i.e.*, equipment owned by competitors (ILECs and CLECs) but sharing the same bays, could be adequately secured. *Order on Reconsideration* at 102. The answer is an unqualified no.

3. Exhibit 1 to this attachment shows a typical equipment aisle, lined on both sides with relay racks in a line-up formation. Commingling would require Verizon to permit a collocater to place its equipment in, for example, the vacant bay

visible in the lower right portion of the image and to access that equipment at its convenience. This picture demonstrates the sheer impossibility of partitioning commingled equipment, which as I conclude in my Declaration, is the only way to secure equipment appropriately.

4. As Exhibit 2 to this attachment illustrates, partitioning does not occupy large amounts of floor space, as the collocators have claimed. To the contrary, the fencing occupies a minimum amount of floor space, but provides the maximum degree of protection. Exhibit 2 further demonstrates that partitioning is a reasonable and unobtrusive method of securing Verizon's network.¹

B. CAMERAS CANNOT PROVIDE ADEQUATE PROTECTION.

5. As I explain in my Declaration, cameras alone do not provide adequate security in a central office environment because there are many obstructions in a central office that would block the view of the camera and make it impossible to determine precisely what a collocator technician was doing. For example, as shown in Exhibit 1, because of the height of equipment lineups, Verizon must place ladders throughout its central offices. A ladder placed between a camera and a technician would obstruct that technician from view and prohibit anyone viewing the image from determining on what equipment the technician was working. Exhibit 3 shows how other obstructions would prevent a camera from capturing a worker's activities.

6. Moreover, Exhibit 1's long shot of an equipment aisle represents the likely placement of a camera because it affords the widest coverage. A camera placed at this distance could not determine in front of which relay rack an individual might be

¹ Please note that this picture was not taken in my presence, but represents my clear recollection of the amount of floor space occupied by partitioning.

standing, much less if he were tampering with equipment or pilfering plug-ins. Exhibits 4 and 5 also illustrate this point. Exhibit 5 shows a technician removing a plug-in from a line-up. A collocator technician could easily remove the plug-in and place it in his pocket without detection.) The slightest angle (*see e.g.*, Exhibit 3) could block the camera's view of the technician. In this picture, the cable riser almost completely obscures the technician from view.

C. ACCIDENTS ARE LIKELY TO INCREASE IN A COMMINGLED ENVIRONMENT.

7. As noted in my Declaration, accidents are likely to occur in a central office because of the narrow aisles separating rows of relay racks. As Exhibits 5 and 6 demonstrate, aisles often have only enough room for a single person to work without a tool belt. Even then, the only way to avoid serious damage to equipment is for technicians to be very careful. As I explain in my Declaration, it is not reasonable to assume that a collocator employee or contractor would exercise the same degree of care when working next to Verizon equipment as a Verizon employee or contractor. As these pictures show, one false move could knock out a service.

D. THEFT IS ALSO LIKELY TO INCREASE IN FREQUENCY.

8. As noted in my Declaration, theft is highly probable in a commingled environment in which numerous individuals, not known by Verizon employees, traipse in and out each day. Not only is there a lucrative secondary market for telecommunications equipment both at home and abroad, but much of this equipment is also used by the collocators.

9. In my visits to the four central offices, I saw many test sets left out in the open (by necessity) and readily available. (*See e.g.*, Exhibit 7). I have been informed that these test sets cost well into the tens of thousands of dollars.

D. PROPRIETARY AND CONFIDENTIAL INFORMATION IS READILY AVAILABLE.

10. As discussed in my Declaration, central office equipment is often labeled with the location of Verizon's customer, primarily to enable technicians to work on the right equipment. *See, e.g.*, Exhibit 8. This allows a collocater to easily determine the identity of the customer served by a piece of equipment. Moreover, as discussed in my Declaration, allowing collocaters access to Verizon equipment would also enable them to determine the addresses of government agencies that prefer not to have their locations known to the public.

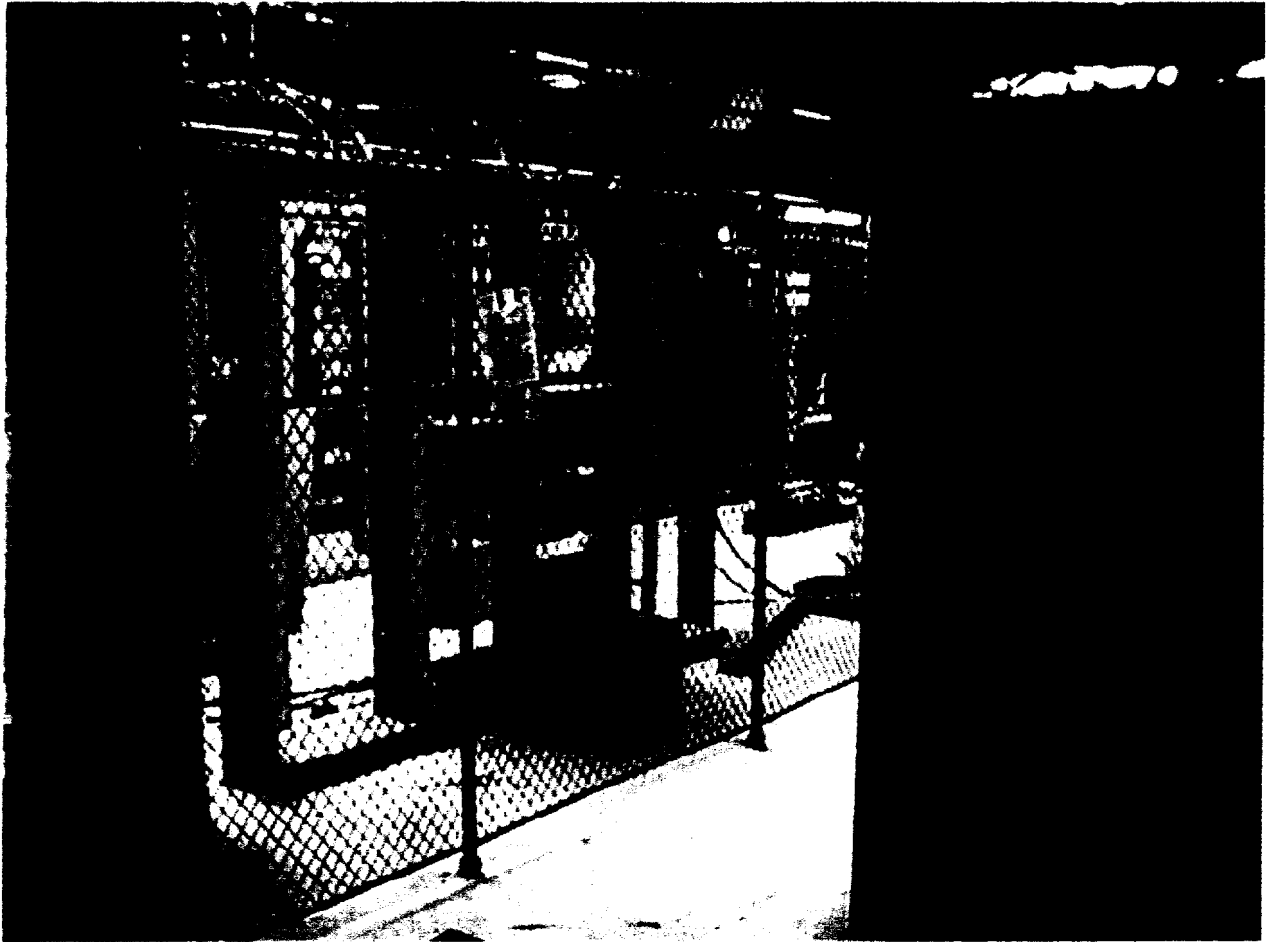
E. REMOTE TERMINALS CAN ONLY BE SECURED WITH PERSONNEL ESCORTS.

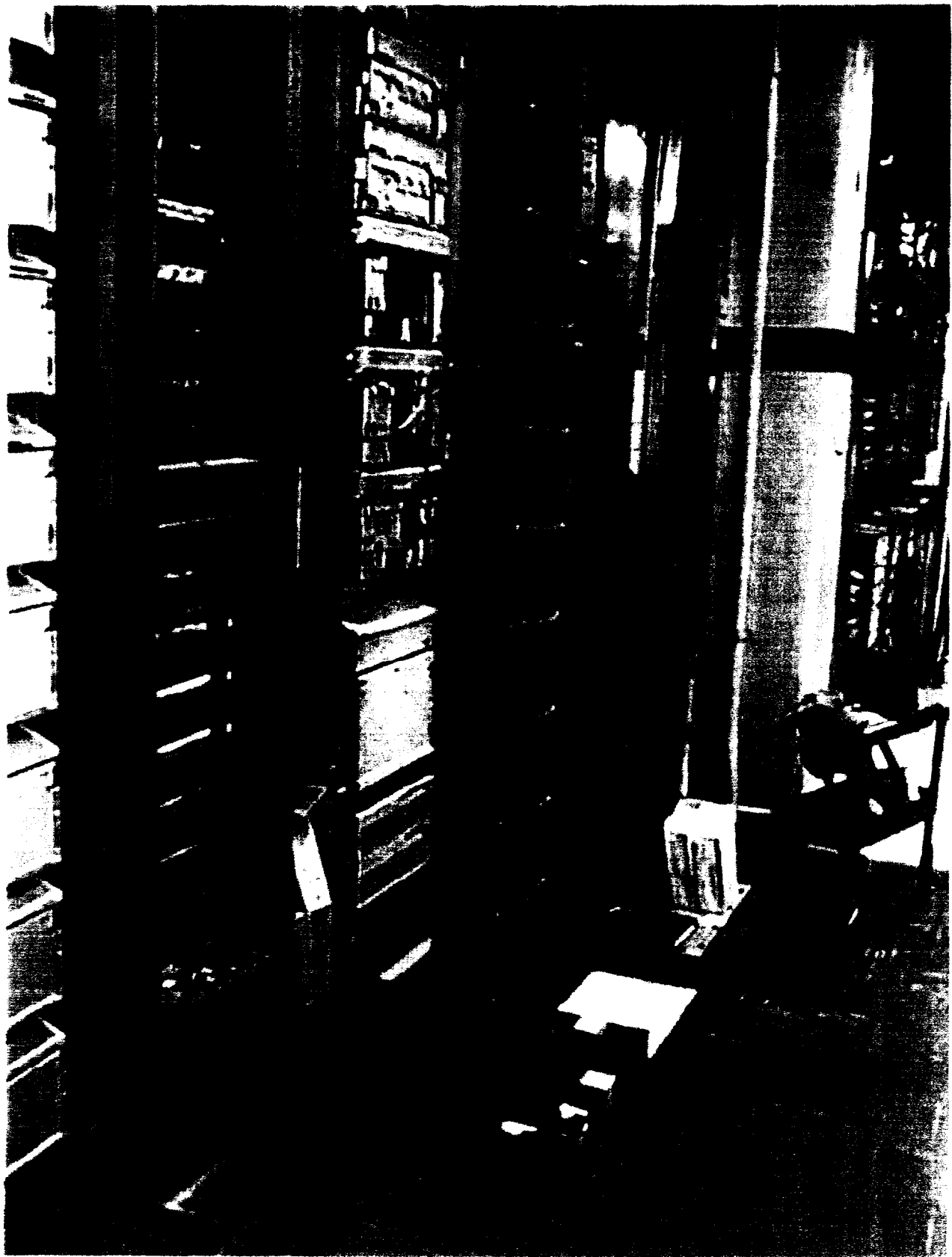
11. Finally, the Commission asked for comment on the security implications of permitting collocaters unfettered access to remote terminals. Exhibit 9 shows the outside of a typical underground controlled environmental vault ("CEV") and Exhibit 10 shows its interior, which is no more than 15' long and 4' wide. These enclosures are tiny structures, often with room for one or two people (at most) at one time. (*See* Exhibit 10). Clearly, partitioning is not an option in such an environment.

12. Moreover, remote terminals come in a variety of shapes and sizes. Exhibits 11 and 12 depict an above-ground cabinet. Allowing CLECs to collocate in these structures would require that Verizon permit them to place equipment literally in between and among its own.

13. In my opinion, the only way to provide adequate security in these situations is to either require a security escort or to limit these structures to virtual collocation. Placing cameras or other forms of security measures would be technically infeasible and cost prohibitive.



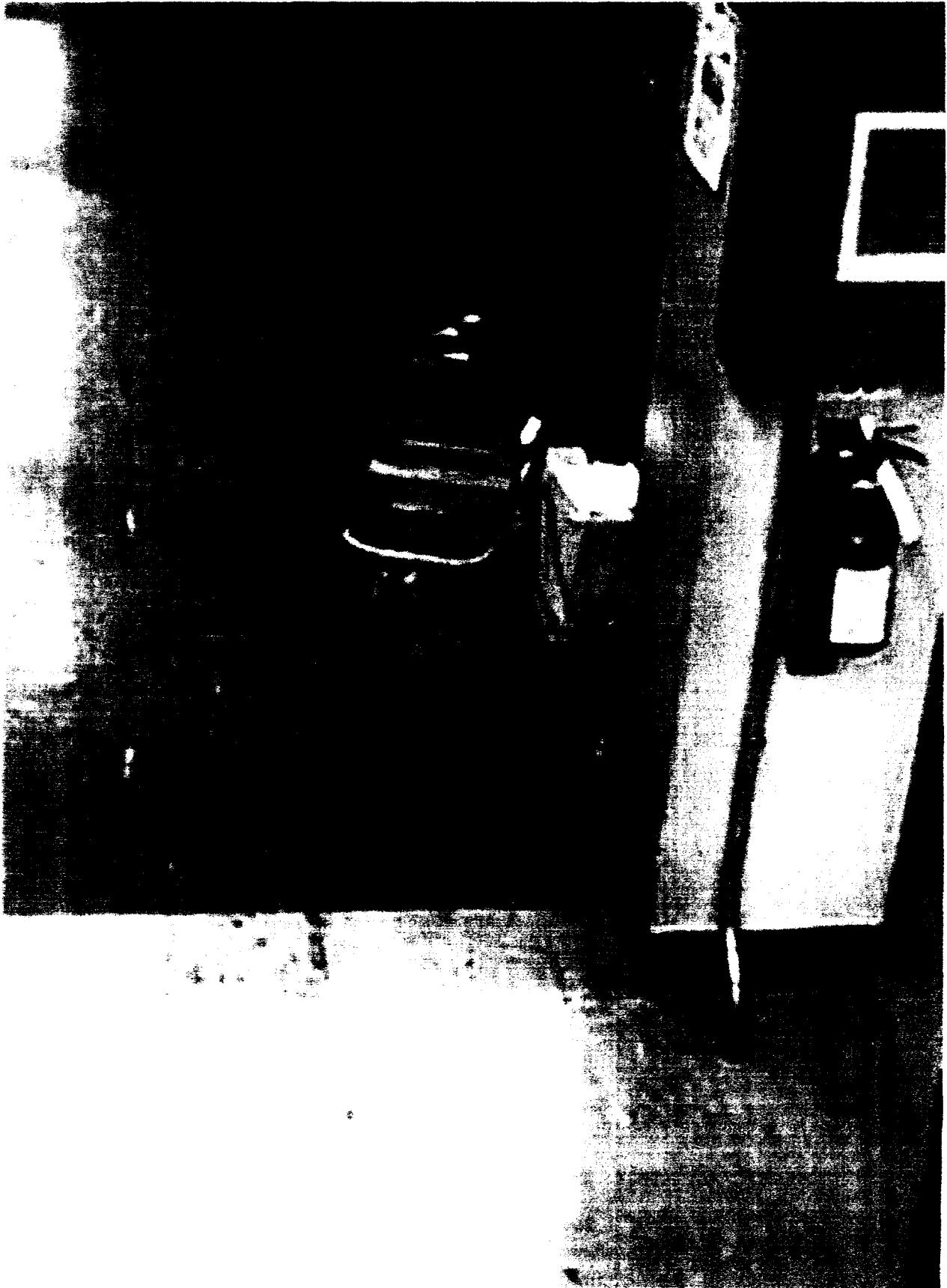












DSC COMMUNICATIONS CORPORATION

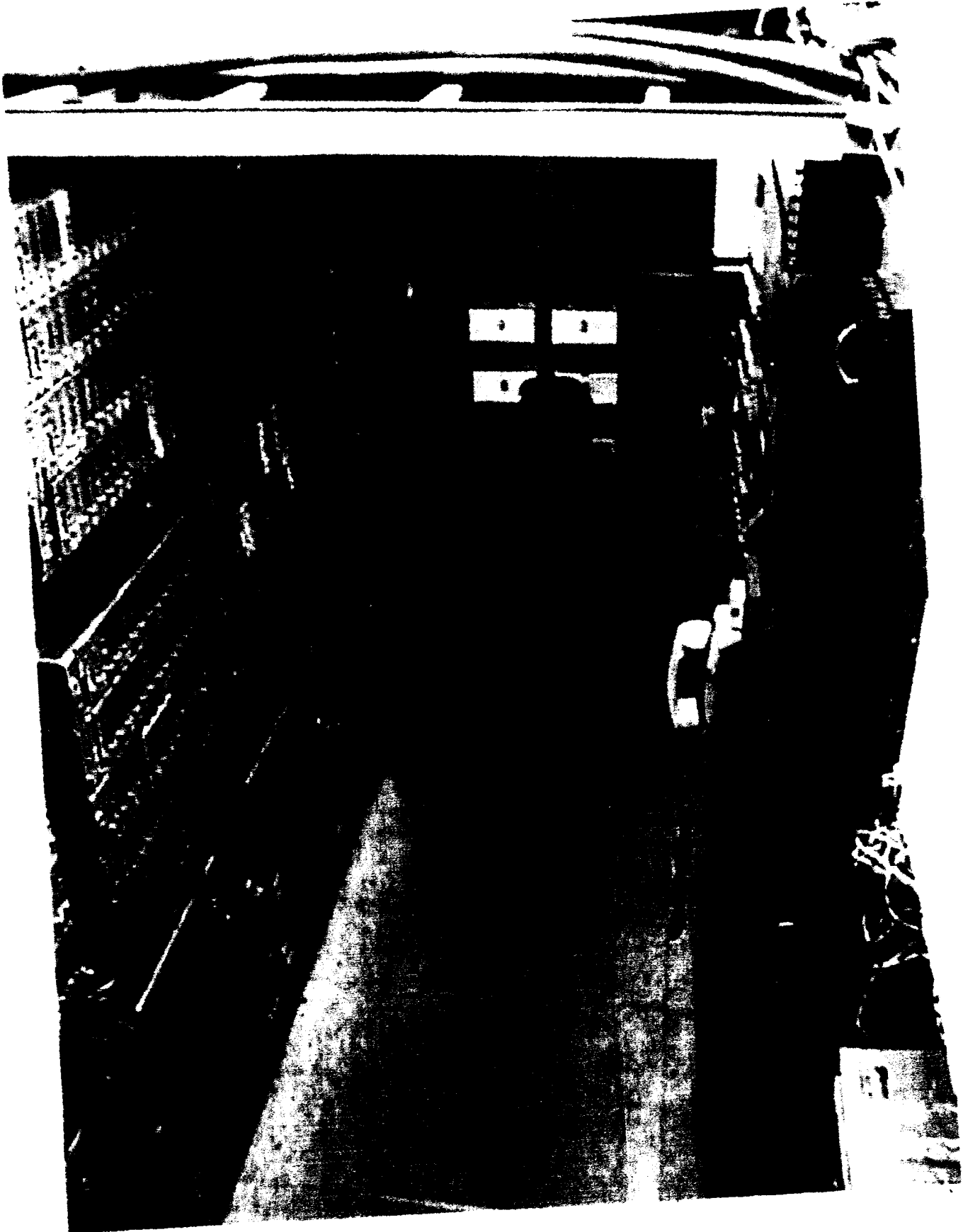
4315 CHAIN BRIDGE RD

FRFXVA 0189 PG 52

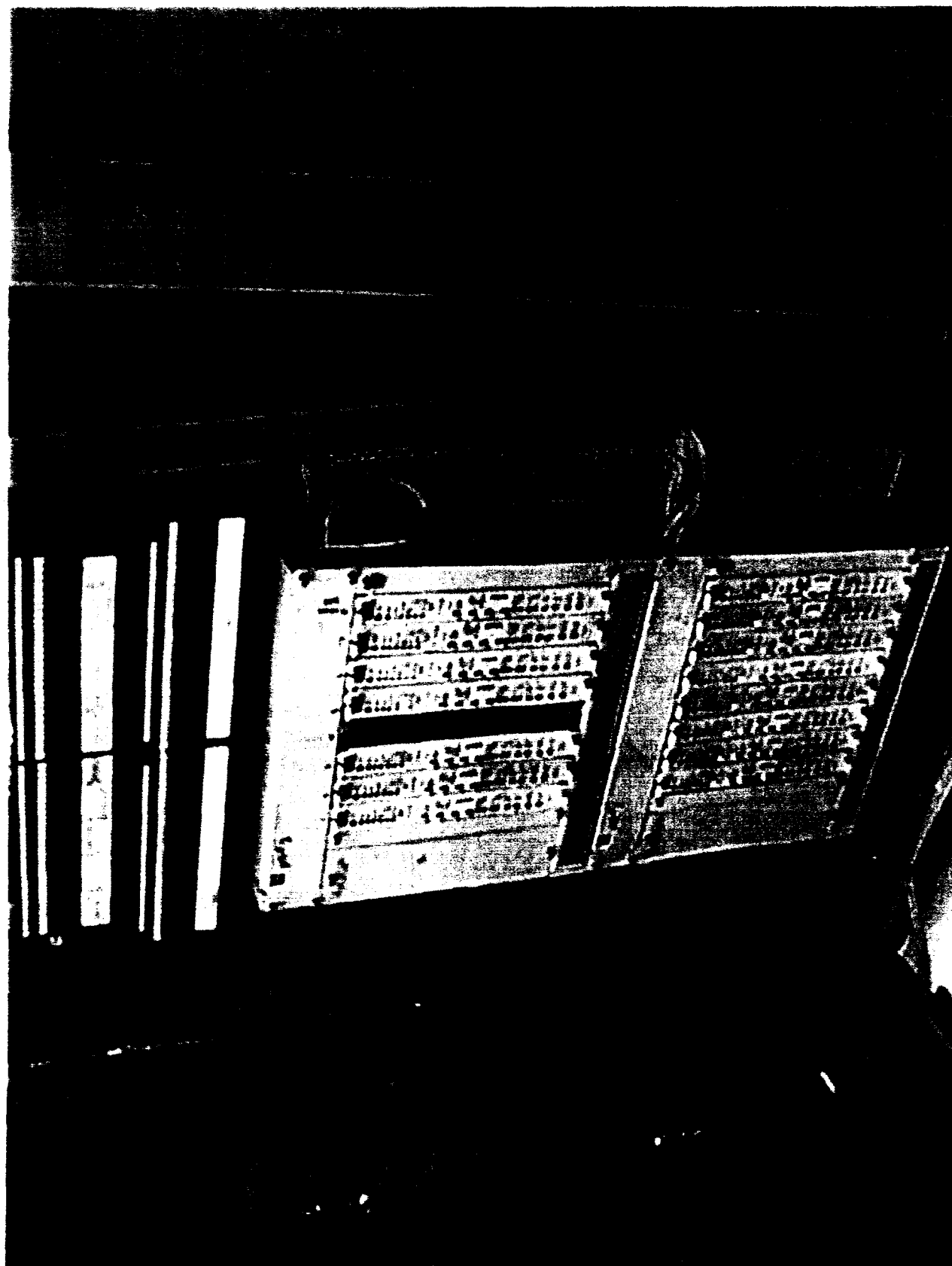
LITESPAN 200

FRFXVA 0189 PG 52









Before the
FEDERAL COMMUNICATIONS COMMISSION
 Washington, D.C. 20554

In the Matter of)	
)	
Deployment of Wireline Services Offering)	CC Docket No. 98-147
Advanced Telecommunications Capability)	
)	
and)	
)	
Implementation of the Local Competition)	CC Docket No. 96-98
Provisions of the Telecommunications)	
Act of 1996)	

ATTACHMENT C-2 TO THE DECLARATION OF DAVID G. MAPLES, III

1. As I mention in my Declaration, partitioning is the only effective method of securing Verizon's equipment and network because it is the only method that prevents security breaches from occurring. I also explain in my Declaration that security cameras alone do not provide adequate security in a central office environment. To further demonstrate these points, I analyze in this Attachment the security measures (and associated costs) that would be necessary in a typical central office if the Commission prohibited Verizon from partitioning its equipment from the CLECs' equipment.

2. Exhibit 1 to this attachment contains the blueprints for an actual Verizon central office from which all identifying detail has been deleted. Managers with responsibility for collocation from Verizon's Corporate Security Group and Real Estate Construction Services Group worked with me to determine the security measures that would be necessary in this central office in a commingled environment.

3. Sheet 1 depicts the basement, which contains the boiler room and mechanical equipment. No telecommunications equipment is located in the basement.

However, because collocators have access to both stair towers on the upper floors, cameras and card readers are necessary to ensure that no unauthorized collocator enters the basement.

4. Sheet 2 depicts the first floor, which is dedicated, in large part, to collocation. As shown, a card reader and camera are required at the entrances to the building and to the interior stairwell. This provides Verizon with some limited ability to identify who enters its building and who uses the stairwell to access other parts of the office once inside. Further, a camera in the stairwell monitors where the collocator travels in the building. An additional card reader permits collocators to access the collocation room.

5. Verizon would place a camera at the entrance to the power room, also housed on the first floor. Because the collocation room is so large, applicable law requires that it have two freely accessible exits. Thus, Verizon would be unable to secure the entrance to the power room with a card reader. Instead, it would have to install a camera to try to detect any unauthorized entrant into the power room. Moreover, in order to restrict access into the collocation room by unauthorized Verizon personnel, Verizon includes a card reader on the door from the power room into the collocation area. As noted above, this door would open freely into the power room to provide a second exit.

6. The second floor, depicted on Sheet 3, houses the switch, which is partitioned from the transport equipment also located on the second floor. The entrance to the switch room is guarded with a card reader and camera to control access and match entrants with access cards. Security cameras and card readers at the room's entrance provide some ability to audit entrants. (Although they are of limited use, as I explain in

my Declaration). Moreover, 25 cameras are required to capture activities on each equipment aisle. (*See also*, Attachment A, Exhibit 1 for the view these cameras would capture). The length of each equipment aisle necessitates two cameras.

7. The third floor, depicted on Sheet 4, houses only transport equipment. Again, card readers and cameras monitor the entrance from the stairwell, and multiple cameras are required to capture activity in the equipment aisles where collocater equipment might be commingled and to monitor the staging area in the upper portion of the drawing.

8. In total, 13 card readers and 99 cameras would be required to attempt to secure Verizon's network in the commingled environment.

9. Card readers have three components – the control panel (the first panel serves six readers and each additional panel serves seven readers), the reader panel located at each secured entrance and the access cards. Verizon has generally presented cost studies for the cost to provide five access cards to each collocater, including the material cost for the card and the labor necessary to program each card individually.

10. The Verizon managers with whom I worked provided the following approximate costs for these components: control panels (\$10,000), reader panels (\$4,000), and five cards (\$90). A single camera server that can serve up to 32 cameras would cost approximately \$30,500 (\$23,000 for the initial server which serves eight cameras, and up to three \$2,500 expansion modules which each extend the server's capacity by eight cameras), while the cameras themselves cost approximately \$4,000 each.

11. Thus, to secure space in the typical central office, the cost is as follows:

2 control panels x \$10,000 per control panel =	\$20,000
13 card reader panels x \$4,000 per card reader panel =	\$52,000
\$90 to provide 5 cards to each CLEC =	\$90
3 camera servers x \$30,500 per camera server =	\$91,500
99 cameras x \$4,000 per camera =	+ \$396,000
TOTAL:	\$559,590

12. The costs in large cities, such as Manhattan – where buildings are typically many stories high – would be much higher. Costs would also be higher in central offices that would require additional security measures to protect the switch, main distributing frame or other crucial network infrastructure.

13. Further, to monitor these cameras and attempt to thwart any illegal action would require a full-time security staff for each of Verizon's more than 5,500 central offices. Four employees at each central office would cost more than \$200,000 per year, or about \$50,000 per employee (plus benefits and overhead),

14. Requiring Verizon to implement these security measures instead of partitioning would greatly increase collocators' costs. Partitioning, on the other hand, costs approximately \$75 per linear foot, plus additional (minimal) costs for doors, locks and the necessary grounding.

